Labstep's Security Overview

At Labstep, data security is a priority in everything we do, and we take it very seriously. Earning and keeping your trust is central for our mission and for our success as a product and a company. We believe that our transparent security policy and confidence that your valuable data is safe with us form the basis for a trustworthy and honest link.

Frameworks and Hosting

Amazon Web Services provide a secure and well-tested foundation

Labstep has a continuous working relationship with Amazon Web Services (AWS), allowing for operating and hosting on the most secure and reliable cloud environment. This cooperation allows Labstep to build on a secure system, quickly detecting, iterating and resolving any issues.

With Labstep's active collaboration with AWS, we are responsible for the server maintenance on the platform, rolling out latest bug fixes and patches without requiring any contribution from your side.

The latest information about how AWS values their security can be found **here: https://aws.amazon.com/security/**

You can also view all AWS certifications such as SOC reports and ISO 27001 **here: https://aws.amazon.com/compliance/**

Network Security

AWS virtual networking allows for private access to production systems

We use AWS virtual networking to establish connections with limited access protected from the public access. Our production systems are only available to approved networks and are always protected from the public internet, ensuring whitelisted traffic by applying multilayered firewalls which are continuously reassessed for security.

Data Encryption

SSL connections and client-specific keys create a safe connection between client and server

Labstep always encrypts any transferred, stored, or processed customer data according to the best standards. Labstep has both Encryption in Transit and full encryption at REST for S3 buckets, RDS database and ElasticSearch index. Our TLS/SSL connections ensure reliable encryption of all data that enters Labstep's servers from the Internet. We use AES-256 encryption to encrypt all the data being stored in Labstep.

Backup and Accessibility

Labstep provides file back up with exceptional durability

At Labstep we utilise the most advanced data backup technologies to minimise the risk of customer data loss. Labstep creates raw files for all images and other data uploaded by our users and stores them in an extremely durable Amazon S3 storage service that offers industry-leading data availability, security and performance. Amazon S3 is a storage service with unmatched durability and support, used by the world's leading organisations. You can find out more about Amazon S3 **here: https://aws.amazon.com/s3/**

Our structured data is stored to the MySQL database adapted to synchronise to a backup. If the database failure occurs, backup can be connected with almost no downtime or data loss. The MySQL database is backed up daily and stored, allowing for a quick and accurate data restoration. We also store our weekly backups for 1 year and store our data in multiple geo-locations to ensure excellent data durability.

info@labstep.com help@labstep.com

Independent Security Audits

Our annual security audits allow for the best protection

Labstep carries out annual security audits to ensure data transparency and integrity are maintained to the highest standards. Third-party security professionals engage in annual grey-box penetration tests to ensure up-to-date security.

Authentication

Easy integration for authentication systems

We facilitate your management system by allowing our clients to use their own existing authentication policies, making management, provisioning, or suspending users easy. Labstep can integrate with our users' existing SAML or Google SSO setups, so that users can sign in using a single login, also integrating their existing two-factor authentication.

Two-Factor Authentication

Additional security layer for your business

Secure your accounts with two-factor authentication to ensure you are the only person that can login, even if your password is compromised.

IP Whitelisting

Controlling access to trusted users

Use IP whitelisting as an extra layer of security to ensure your data can only be accessed from specific approved IP addresses.

Compliance

Labstep effectuates strict compliance to regulatory standards

Labstep strictly follows the regulatory compliance by FDA 21 CFR Part 11 through carrying out thorough audit trails, electronic signatures and electronic records support. The security practices used by Labstep comply with FIPS 200 and ISO27001. Additionally, Labstep can make you compliant with Good Laboratory Practice guidelines and Good Manufacturing Guidelines.

OWASP top 10

Labstep has adopted this documentation and mitigates these risks. The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. Find out more here .

Our Team

Labstep is created by top scientists and engineers

Labstep prides itself on the excellent team of scientists and engineers who have precisely designed Labstep based on the world's best industry and technology practices. Our dedicated team of engineers constantly works on enhancing the current security systems, as well as evaluating the risks and trends in data security.

More Information

Labstep welcomes any questions and concerns about data security and privacy. We are dedicated and confident to ensure Labstep aligns with your company's security requirements. For more information, please contact **info@labstep.com.**